SOUTH AFRICAN
CIVIL AVIATION AUTHORITY

Centralised Occurrence Reporting System

GUIDELINES FOR REPORTING OF OCCURRENCES

Aviation Security Management

NOTIFICATION OF MANDATORY AND VOLUNTARY AVIATION SECURITY INFORMATION

1. EXPLANATORY STATEMENT

Subject: Aviation Security (Incident Reporting) Instrument 2020

The Civil Aviation Act, 2009 (Act No. 13 of 2009) established a regulatory framework to safeguard against unlawful interference with aviation. The Civil Aviation Regulations, 2011 (set out in Part 111.01.11 (1) and (2)) require the reporting of aviation security incidents.

The South African Civil Aviation Authority has established a confidential voluntary reporting system (Central Safety and Security Reporting System) for the reporting of information concerning incidents of unlawful interference, by entities responsible for the implementation of the National Aviation Security Programme (NASP), to the Civil Aviation Authority. The system allows anybody to submit Mandatory, Voluntary and Confidential incidents reports.

The system also provides for the gathering and analysis of information on aviation security from sources outside the quality control system, such as reports on a voluntary basis from passengers, crew members and staff employed by airport and aircraft operators.

1.1. Purpose

The purpose of the system is to contribute to the enhancement of the aviation safety and security in South Africa by providing a centralised approach to safety and security for all individuals employed in, or associated with the industry, including the travelling public.

The aim of the reporting system is to contribute to the enhancement of aviation security in South Africa by providing a centralised system to capture security incidents in an effective and efficient manner, to protect and manage information, and to maintain the confidentiality of the information of the person submitting the anonymous or voluntary reports.

This document sets out the information that must be included in a report to the Civil Aviation Authority's data collection and analysis system. Information contained in such reports allows the SACAA to capture and efficiently monitor aviation security incidents. The reports also provide information to enable the State to comply with its international obligations to report aviation security incidents to the International Civil Aviation Organization.

2. REPORTING OF AVIATION SECURITY INFORMATION

2.1. Voluntary incident reports

The system provides for the confidential gathering of information from sources outside the quality control system, such as reports on a voluntary basis from passengers, crew members and staff employed by airport and aircraft operators, for analysis by the authority. Information provided will be handled as confidential and protected.

2.2. Mandatory Reporting of Information Concerning Incidents of Unlawful Interference

2.2.1. The following aviation entities:

(a) designated airport;
(b) air carrier operator of a scheduled service;
(c) ANSP;
(d) catering stores;
(e) catering supplies and
(f) ground handling service provider.

2.2.2. **Definitions - Note**: It is important that persons submitting reports keep the definition of an incident firmly in mind when deciding whether to submit information. If in doubt, the information should still be submitted.

Acts of unlawful interference

These are acts or attempted acts that jeopardize the safety of civil aviation, including but not limited to unlawful seizure of aircraft, destruction of an aircraft in service, hostage-taking on board an aircraft or on aerodromes, forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility, introduction of weapons or hazardous devices or material for criminal purposes and the communication of false information that jeopardize the safety of an aircraft in flight or on the ground; of passengers, crew, ground personnel or the general public, at an airport or on the premises of civil aviation facilities.

Aviation Security Breach

Any incident involving unauthorised and uncontrolled access by an individual or prohibited item into a sterile area or secured area of an airport that presents an immediate and significant risk to life, safety, or the security of the aircraft or airport

Aviation Security Incidents

An aviation security incident is an actual, attempted, threatened or suspected unlawful act, which would cause an interference, breach or malfunction of the civil aviation security system.

Dangerous goods accident

An occurrence associated with and related to the transport of dangerous goods by air, which results in fatal or serious injury to a person or major property damage.

Dangerous goods incident

An occurrence other than a dangerous goods accident associated with and related to the transport of dangerous goods by air, not necessarily occurring on board an aircraft, which results in injury to a person, property damage, fire, breakage, spillage, leakage of fluid or radiation or other evidence that the integrity of the packaging has not been maintained. Any occurrence relating to the transport of dangerous goods that seriously jeopardizes an aircraft, or its occupants, is also deemed to be a dangerous goods incident.

Security Investigation

An inquiry into any act or attempted act of unlawful interference against aviation and/or any alleged or suspected instance of non-compliance with the State's National Civil Aviation Security Programme or other Legal and/or regulatory requirements pertaining to Civil Aviation Security.

2.2.3. Once any breach of the requirements contained in the NASP or any security incident is identified, a report must be made to SACAA as soon as possible, but no later than 48 hours after the security incident is identified.

2.2.4. The information includes, for example, the date, time and location of the aviation security incident; the name of the person reporting the incident; the aviation industry participant to whom the incident directly relates; and a description of the incident, including an indication of whether the incident was a threat of unlawful interference with aviation or an unlawful interference with aviation.

2.2.5. If, at the time of making the report, the industry participant does not have any of the above information, but later attains it, this information must be passed to SACAA by one of the methods contained below, but no later than 24 hours after attaining the information.

The report must be made by using one of the following methods:

(a) Verbal via phone, followed by

(b) Online by e-service (Occurrence Reporting Tool) or
(c) By email Smart PDF.

3. PROCEDURES FOR REPORTING

3.1. E-Service

On-line reporting applications are mostly for individuals, or small/medium organisations), the large organisations are urged to use the E-system.

Start: The process is triggered when a Security Breach Reported is submitted through the SACAA's online / web incident reporting system. A Username will be created for all licence and certificate holders. This process can also be used for voluntary incident reporting.

The reporter logs in and submits the report through the internet service and attaches any supplementary documentation.

3.2. Smart PDF

Acceptable means available to facilitate compliance: Off-line reporting form (mostly for individuals, small/medium organisations).
The operator submits the incident report by completing the aviation security breach reporting form and submits it to the SACAA, using the email AvsecBreachesReporting@caa.co.za.

3.3. Telephone

The operator reports the incident telephonically to the authorised officer.
The authorised officer registers the incident on the online reporting application.

4. GUIDELINES FOR REPORTING OF AVIATION SECURITY BREACH

4.1.1. The following information must be included in the report:

(a) the name, contact number, and email address for the person making the report;
(b) the title or position held by the person making the report;
(c) the name of the employer of the person making the report (where applicable);
(d) the date of the report;
(e) the date and time when the security incident commenced;
(f) the date and time when the security incident ceased;
(g) the location of the security incident (including, where applicable, the name and address of the location where the security incident occurred);
(h) the industry participant or participants to whom the security incident directly relates;

(i) the industry participant or participants who are affected as a result of the security incident;
(j) a detailed description of the security incident, including an indication as to whether the incident was:
    (i) **a threat of unlawful interference; or**
    (ii) **an unlawful interference; and**
(k) if the security incident was a threat of unlawful interference:
(i) the name and contact details of the person who received the threat;
(ii) the details of the threat;
(iii) whether the person making the report assessed the threat as genuine or as a hoax and how they made that assessment; and
(iv) whether discovering who made the threat was successful, unsuccessful, ongoing or not attempted; and
(l) if the security incident involved an aircraft:
    (i) the aircraft type;
    (ii) the flight number;
    (iii) whether or not the aircraft was in flight at the time of the security incident; and
    (iv) the type of cargo on board (if applicable);
(m) if the security incident involved a building or other infrastructure, information sufficient to identify the building or other infrastructure, such as the building number or other identifier;
(n) if the person making the report is aware that the security incident has previously been reported to the SACAA:
    (i) the approximate time and date at which the security incident was reported; and
    (ii) the name or position of the person, or the name of the department in the SACAA, to whom the incident was reported;
(o) if the security incident has been reported to the police, an industry participant or any other body:
    (i) the approximate time and date at which the security incident was reported; and
    (ii) the name and contact information of the person the incident was reported to;

(p) whether the report is the result of a routine security inspection;
(q) if the report is the result of a security incident being brought to the attention of the person making the report by a third party:
    (ii) that the report is the result of notification from a third party; and
    (iii) the name, and where applicable, name of the employer, of the third party; and
(r) the steps that the industry participant has taken, or is in the process of taking, to ensure that the security incident does not occur again.

INVESTIGATION

The reporting, analysis and follow-up of security breaches are enhanced by a broader security risk management process that helps to identify the main security issues. This process involves continuous communication between the industry and the authority as part of routine security management activity. This includes the provision of feedback and lessons learned, to counter the identified threat and risk, to improve safety and security.

4.2. The system automatically notifies the receipt of the report through the email to the system administrator, who will assess the risk and save the incident. The system generates the incident report number and the incident will be allocated to the authorised officer for investigation.

4.3. The system administrator will submit an email notification to the client to acknowledge receipt and share the incident number and the name of the authorised officer responsible for investigation of the reported incident.

4.4. The authorised officer in charge of the reported incident reviews the report and the attachments, where applicable.

4.5. If more information is required to start the investigation of the event, the authorised officer will contact the reporter and request more details and/or relevant documents.

4.6. The reporter receives the email and/or the notification email and submits the requested information and/or documents.

4.7. If all the required information and documents are received and available, the authorised officer starts the investigation.

4.8. The authorised officer reviews and analyses all elements related to the submitted report and evidence and compiles and submits the investigation report with the recommendations to the Manager.

4.9. Based on the investigation report and recommendations, the Manager convenes a meeting with the affected departmental leaders and discusses the report, updates the risk register, corresponds with the operator (submitter of the incident report), and closes the case.

End of Process